

EXHIBIT 1

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF A
GRAY 2022 TOYOTA CAMRY WITH
VEHICLE IDENTIFICATION NUMBER
4T1S11BK8NU072229 AND MICHIGAN
LICENSE PLATE ESB3341 CURRENTLY
LOCATED AT THE ANDROSCOGGIN
COUNTY SHERIFF'S OFFICE

No. 2:24-mj-00009-KFW

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jonathan Duquette, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of a gray 2022 Toyota Camry with Vehicle Identification Number 4T1S11BK8NU072229 and Michigan license plate ESB3341 (hereafter the “Target Vehicle”) which is currently in law enforcement possession. Items to be seized are described in Attachment B1.

2. I am a Task Force Officer with the Federal Bureau of Investigation (FBI). I have been in this position since June 2015, and I have been a Task Force Officer in FBI’s Boston Division since January 2018. I am also a Border Patrol Agent with the U.S. Border Patrol and have been in this position since December 2009. In my career, I have utilized various investigative tools and techniques, to include the use of search warrants.

3. This affidavit is intended to provide the facts necessary for a determination of probable cause for the requested search warrant.

4. The applied-for warrant would authorize the forensic examination of any electronic devices located inside the Target Vehicle for the purpose of identifying electronically stored data particularly described in Attachment B2.

PROBABLE CAUSE – HOME INVASION

5. I know from my review of reports and from conferring with law enforcement officers that on about January 3, 2024, at approximately 1:00 a.m., the Androscoggin County Sheriff's Office received a 911 emergency call requesting that police respond to 79 Longley Road in Greene. As reported in the call, an unknown man had forced his way into the residence with a handgun.

6. As detailed in police reports, the occupants of 79 Longley Road had overpowered and subdued the intruder while they waited for authorities to arrive. By approximately 1:55 a.m., deputies from the Androscoggin County Sheriff's Office had arrested the intruder, who they were able to identify as Target Subject SCOTT HAFFORD. Deputies learned from Maine Bureau of Motor Vehicles (BMV) records that HAFFORD resided at 259 Taber Hill Road, Vassalboro, Maine (the "Subject Residence"). Deputies learned that HAFFORD had kidnapped a woman from her home, located at 98 Longley Road in Greene, before forcing her to go with him to a neighbor's house. Once at the neighbor's house (79 Longley Road), HAFFORD forced the women to knock on the door to get the homeowner to answer. Once they did, HAFFORD forced his way into the house with a handgun. Deputies ultimately recovered a Smith and Wesson Bodyguard .380 caliber handgun with serial number KFV6229 from the scene.

7. Deputies interviewed one of the owners of 79 Longley Road, who reported that she had noticed a vehicle in the driveway that did not belong to her or anyone in her

family. She assumed it belonged to HAFFORD. The homeowner opened the vehicle's door and saw a phone and a tablet. The homeowner touched both electronic devices. The vehicle was later identified as the Target Vehicle. The Target Vehicle was later towed from the scene and impounded at the Androscoggin County Sheriff's Office pending a search warrant application.

8. A check of police databases for Target Subject SCOTT HAFFORD revealed that he was on active bail conditions for operating under the influence and two counts of terrorizing. Among other provisions, the bail conditions specified that HAFFORD was not to use or possess illegal drugs, alcohol, dangerous weapons, or firearms.

9. A check of HAFFORD's criminal history showed that he was sentenced for two prior felonies and a prior misdemeanor domestic assault, each of which would independently make him prohibited from lawful possession of a firearm. HAFFORD was convicted of (1) felony tampering with a witness, information, juror or victim on March 17, 2011, for which he received a sentence of six years' incarceration all suspended (ALFSCCR201001778); (2) felony eluding on March 17, 2011, for which he received a sentence of 364 days incarceration (ALFSCCR201001777); (3) domestic violence assault (misdemeanor) on January 14, 2013, for which he received a sentence of 364 days all but 15 days suspended (AUGDCCR201300106).

10. Based upon the home invasion described above, HAFFORD was charged in ten-counts by complaint in Androscoggin County District Court as follows: Count 1: Kidnapping, Counts 2 & 3: Burglary, Count 4: Possession of a firearm by a prohibited person, Counts 5, 6, & 7 Criminal threatening with a dangerous weapon, Counts 8 & 9: Assault, and Count 10: Violation of conditions of release.

PROBABLE CAUSE – CHILD SEXUAL ABUSE MATERIAL

11. In the course of investigating the home invasion for possible federal adoption, on or about January 10, 2024, I learned that the Maine State Police Computer Crimes Unit (CCU) had executed a search warrant at the Subject Residence on about January 8, 2024, as part of a Child Sexual Abuse Material (CSAM) investigation.

12. I have reviewed the search warrant authorizing the January 8, 2024 search, from which I have learned the following, in substance and in part:

a. On December 1, 2023, the CCU received a CyberTip from the National Center for Missing and Exploited Children (NCMEC). NCMEC CyberTip line Report Number 179317354 was submitted by Electronic Service Provider (ESP) Dropbox in accordance with federal law, 18 U.S.C.A. § 2258A.

b. NCMEC is a nonprofit organization that provides services to families and professionals that relate to the abduction and sexual exploitation of children. NCMEC also operates the CyberTip line and the Child Victim Identification Programs to assist law enforcement officers and others in identifying and rescuing victims of child exploitation and child pornography. As part of the NCMEC directives, the NCMEC works with electronic service providers (ESP) and remote computing service providers, such as Facebook, to reduce the dissemination of child pornography images and videos on the internet. When an ESP becomes aware of suspected child pornography, the ESP representative may view the items in question to determine if they are child pornography, and therefore constitute a violation of the ESP use agreement with its user(s). If the subject media are deemed by the ESP representative to be child pornography, the ESP will file an electronic report with the NCMEC. The

reporting ESP will provide in the NCMEC report samples of the child pornography itself, IP addresses¹ captured at the date and time of the child pornography file being uploaded by the user, and any registration information (if available). NCMEC will then research more publicly available information based on the information provided to it by the ESP to determine, if possible, the identification and or geographic location of the user uploading the child pornography in order to forward the report to the appropriate jurisdiction. NCMEC will then forward its report to the Regional Internet Crimes Against Children (ICAC) commander for further investigation. The Maine Computer Crimes Unit is the regional ICAC for Maine.

c. In CyberTip # 179317354, the ESP Dropbox did view the entire content of one video file of reported sexually explicit material. The NCMEC CyberTip report indicated that NCMEC also viewed the content, as they were identified by hash value.

d. On December 1, 2023, a CCU Criminal Intelligence Analyst began an investigation into CyberTip # 179317354 and learned that a Dropbox account assigned to email address “v6hvq8fkr2@privaterelay.appleid.com” had uploaded one video file of a child being sexually exploited. The incident date and time provided by

¹ *Internet Protocol Number (IP)* An IP is a unique numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 (IPv4), and 2001:db8:0:1234:0:567:8:1 (IPv6). Every machine that is on the Internet has an IP number. Every location has a unique IP number.

Dropbox was November 8, 2023, at 02:16:01 hours Universal Time Coordinated (UTC²).

The connection log provided by Dropbox identified the IP address used during that date and time was 2603:7081:6dfo:6780:e4c1:c511:1894:de9 (the “Subject IP Address”).

Research on the Subject IP Address through an open-source Geographic Locator called MaxMind (www.maxmind.com) listed an approximate geographic location of Vassalboro, Maine, with the internet service provider (ISP) being Spectrum, also known as Charter Communications.

e. CCU obtained a subpoena for subscriber information for the Subject IP Address for November 8, 2023 at 02:16:01 hours UTC. On December 8, 2023, Charter Communications responded and indicated the subscriber on the account was N.D. with an address of 259 Taber Hill Rd, Vassalboro, Maine (i.e., the Subject Residence). They also provided a telephone number ending in 3607.

f. CCU searched a commercially available, subscription-based database service for N.D. Through this search, Target Subject SCOTT HAFFORD was identified as also being associated with the Subject Residence.

g. On January 4, 2024, a CCU Detective reviewed the file captured by Dropbox that was provided in the CyberTip report # 179317354 and determined that the video would qualify as sexually explicit material under Maine law. More specifically, the video file with the name “4029824525618326838.MP4” depicted a girl between 7-9

² UTC is Coordinated Universal Time and widely used as a standard worldwide clock. It had replaced Greenwich Mean Time. Eastern Standard Time (EST) is four or five hours less than UTC depending on Daylight Savings Time.

years of age, wearing only a t-shirt. The female child was being recorded along with an adult female who was masturbating while the female child was fondling and licking the adult female's breast. The child's age was estimated based on body growth and development. A screen shot of the video file was captured.

h. The CCU Detective researched Target Subject HAFFORD and N.D. through the BMV, which showed they are both associated with the Subject Residence.

13. I know from my review of police reports, and through discussion with officers, that on about January 8, 2024, members of the CCU executed the search warrant at the Subject Residence. During the execution of the search warrant, N.D. was present. N.D. said HAFFORD was currently incarcerated at the Androscoggin County Jail. N.D. pointed out various electronic devices in the residence and said she believed HAFFORD last left the residence with his blue cellphone and a black tablet. A computer forensic Analyst conducted an on-scene search of N.D.'s cellphone for child pornography, which was not detected. N.D.'s cellphone was the only device examined on scene. N.D. said HAFFORD could have had other devices or electronic storage devices without her knowing about them.

14. N.D. told officers that she was not familiar with Dropbox, or the email address of "v6hvq8fkr2@privaterelay.appleid.com." N.D. stated that she and HAFFORD lived at the residence alone for nearly 8 years and their internet was password protected. N.D. said she had no knowledge of anyone else using their internet service. N.D. said several times if someone was looking up sexual images of children it had to be HAFFORD. N.D. said the last time she saw or spoke to HAFFORD was when

he left the residence the morning of his arrest. N.D. said she was unsure of what HAFFORD was driving when he was arrested for a home invasion.

15. I have learned from the Androscoggin County Sheriff's Office that a rental vehicle had been impounded on January 3, 2024, and that the rental vehicle had been used by HAFFORD during the home invasion described above. Androscoggin County Detective Sergeant Drouin reported that he observed a cellphone and a black tablet inside the rental vehicle. The rental vehicle was later identified as the Target Vehicle.

16. A registration query search through the BMV on the Target Vehicle indicated the registered owner is EAN Holdings (i.e., Enterprise Rent-A-Car). An Enterprise Rent-A-Car employee from the rental location informed law enforcement that HAFFORD rented the Target Vehicle on January 2, 2024, and that the vehicle had not been returned. HAFFORD provided a Maine driver's license and a credit card at the time of the rental.

TECHNICAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad

range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts

of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many

of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

18. Based on my training, experience, and research, I believe that the devices located inside the Target Vehicle have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, websites and other content that have been viewed via the Internet are typically stored for some period of time on the accessing device. This information can sometimes be recovered with forensics tools.

20. *Forensic evidence.* As further described in Attachment B2, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic

evidence that establishes how the devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

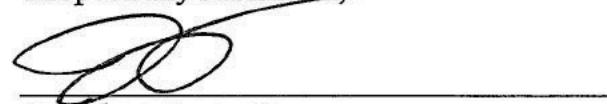
21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I submit that this affidavit supports probable cause for a search warrant authorizing the search of the Target Vehicle to seek items described in Attachment B1. I also submit this affidavit supports probable cause for a search warrant to search any electronic devices or media located in the Target Vehicle to seek the items described in Attachment B2.

Respectfully submitted,



Jonathan Duquette
Task Force Officer
Federal Bureau of Investigation

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedures

Date: Jan 19 2024

City and state: Portland, Maine

